



# **Configurare la rete**

## **Cloud Manager 3.8**

NetApp  
March 25, 2024

# Sommario

- Configurare la rete ..... 1
  - Requisiti di rete per Cloud Volumes ONTAP in AWS ..... 1
  - Configurazione di un gateway di transito AWS per coppie ha in più AZS ..... 8
  - Regole del gruppo di sicurezza per AWS ..... 12

# Configurare la rete

## Requisiti di rete per Cloud Volumes ONTAP in AWS

Configurare la rete AWS in modo che i sistemi Cloud Volumes ONTAP possano funzionare correttamente.

### Requisiti generali per Cloud Volumes ONTAP

I seguenti requisiti devono essere soddisfatti in AWS.

#### Accesso a Internet in uscita per nodi Cloud Volumes ONTAP

I nodi Cloud Volumes ONTAP richiedono l'accesso a Internet in uscita per inviare messaggi a NetApp AutoSupport, che monitora in modo proattivo lo stato di salute dello storage.

I criteri di routing e firewall devono consentire il traffico HTTP/HTTPS di AWS ai seguenti endpoint in modo che Cloud Volumes ONTAP possa inviare messaggi AutoSupport:

- <https://support.netapp.com/aods/asupmessage>
- <https://support.netapp.com/asupprod/post/1.0/postAsup>

Se si dispone di un'istanza NAT, è necessario definire una regola del gruppo di sicurezza in entrata che consenta il traffico HTTPS dalla subnet privata a Internet.

["Scopri come configurare AutoSupport"](#).

#### Accesso a Internet in uscita per il mediatore ha

L'istanza di ha mediator deve disporre di una connessione in uscita al servizio AWS EC2 in modo che possa fornire assistenza per il failover dello storage. Per fornire la connessione, è possibile aggiungere un indirizzo IP pubblico, specificare un server proxy o utilizzare un'opzione manuale.

L'opzione manuale può essere un gateway NAT o un endpoint VPC di interfaccia dalla subnet di destinazione al servizio AWS EC2. Per ulteriori informazioni sugli endpoint VPC, fare riferimento a ["Documentazione AWS: Endpoint VPC di interfaccia \(AWS PrivateLink\)"](#).

#### Numero di indirizzi IP

Cloud Manager assegna il seguente numero di indirizzi IP a Cloud Volumes ONTAP in AWS:

- Nodo singolo: 6 indirizzi IP
- Coppie HA in un singolo AZS: 15 indirizzi
- Coppie HA in più AZS: 15 o 16 indirizzi IP

Si noti che Cloud Manager crea una LIF di gestione SVM su sistemi a nodo singolo, ma non su coppie ha in un singolo AZ. È possibile scegliere se creare una LIF di gestione SVM su coppie ha in più AZS.



LIF è un indirizzo IP associato a una porta fisica. Per strumenti di gestione come SnapCenter è necessaria una LIF di gestione SVM.

## Gruppi di sicurezza

Non è necessario creare gruppi di sicurezza perché Cloud Manager fa questo per te. Se è necessario utilizzare il proprio, fare riferimento a ["Regole del gruppo di sicurezza"](#).

## Connessione da Cloud Volumes ONTAP ad AWS S3 per il tiering dei dati

Se si desidera utilizzare EBS come Tier di performance e AWS S3 come Tier di capacità, è necessario assicurarsi che Cloud Volumes ONTAP disponga di una connessione a S3. Il modo migliore per fornire tale connessione consiste nella creazione di un endpoint VPC per il servizio S3. Per istruzioni, vedere ["Documentazione AWS: Creazione di un endpoint gateway"](#).

Quando si crea l'endpoint VPC, assicurarsi di selezionare la regione, il VPC e la tabella di routing che corrispondono all'istanza di Cloud Volumes ONTAP. È inoltre necessario modificare il gruppo di protezione per aggiungere una regola HTTPS in uscita che abilita il traffico all'endpoint S3. In caso contrario, Cloud Volumes ONTAP non può connettersi al servizio S3.

In caso di problemi, vedere ["AWS Support Knowledge Center: Perché non è possibile connettersi a un bucket S3 utilizzando un endpoint VPC gateway?"](#)

## Connessioni a sistemi ONTAP in altre reti

Per replicare i dati tra un sistema Cloud Volumes ONTAP in AWS e i sistemi ONTAP in altre reti, è necessario disporre di una connessione VPN tra AWS VPC e l'altra rete, ad esempio Azure VNET o la rete aziendale. Per istruzioni, vedere ["Documentazione AWS: Configurazione di una connessione VPN AWS"](#).

## DNS e Active Directory per CIFS

Se si desidera eseguire il provisioning dello storage CIFS, è necessario configurare DNS e Active Directory in AWS o estendere la configurazione on-premise ad AWS.

Il server DNS deve fornire servizi di risoluzione dei nomi per l'ambiente Active Directory. È possibile configurare i set di opzioni DHCP in modo che utilizzino il server DNS EC2 predefinito, che non deve essere il server DNS utilizzato dall'ambiente Active Directory.

Per istruzioni, fare riferimento a ["Documentazione AWS: Active Directory Domain Services su AWS Cloud: Implementazione di riferimento rapido"](#).

## Requisiti per coppie ha in più AZS

Ulteriori requisiti di rete AWS si applicano alle configurazioni Cloud Volumes ONTAP ha che utilizzano zone di disponibilità multiple (AZS). Prima di avviare una coppia ha, è necessario esaminare questi requisiti perché è necessario inserire i dettagli di rete in Cloud Manager.

Per informazioni sul funzionamento delle coppie ha, vedere ["Coppie ad alta disponibilità"](#).

## Zone di disponibilità

Questo modello di implementazione ha utilizza più AZS per garantire un'elevata disponibilità dei dati. È necessario utilizzare un AZ dedicato per ogni istanza di Cloud Volumes ONTAP e per l'istanza del mediatore, che fornisce un canale di comunicazione tra la coppia ha.

## Indirizzi IP mobili per dati NAS e gestione cluster/SVM

Le configurazioni HA in più AZS utilizzano indirizzi IP mobili che migrano tra nodi in caso di guasti. Non sono accessibili in modo nativo dall'esterno del VPC, a meno che non si ["Configurare un gateway di transito AWS"](#).

Un indirizzo IP mobile è per la gestione del cluster, uno per i dati NFS/CIFS sul nodo 1 e uno per i dati NFS/CIFS sul nodo 2. Un quarto indirizzo IP mobile per la gestione SVM è opzionale.



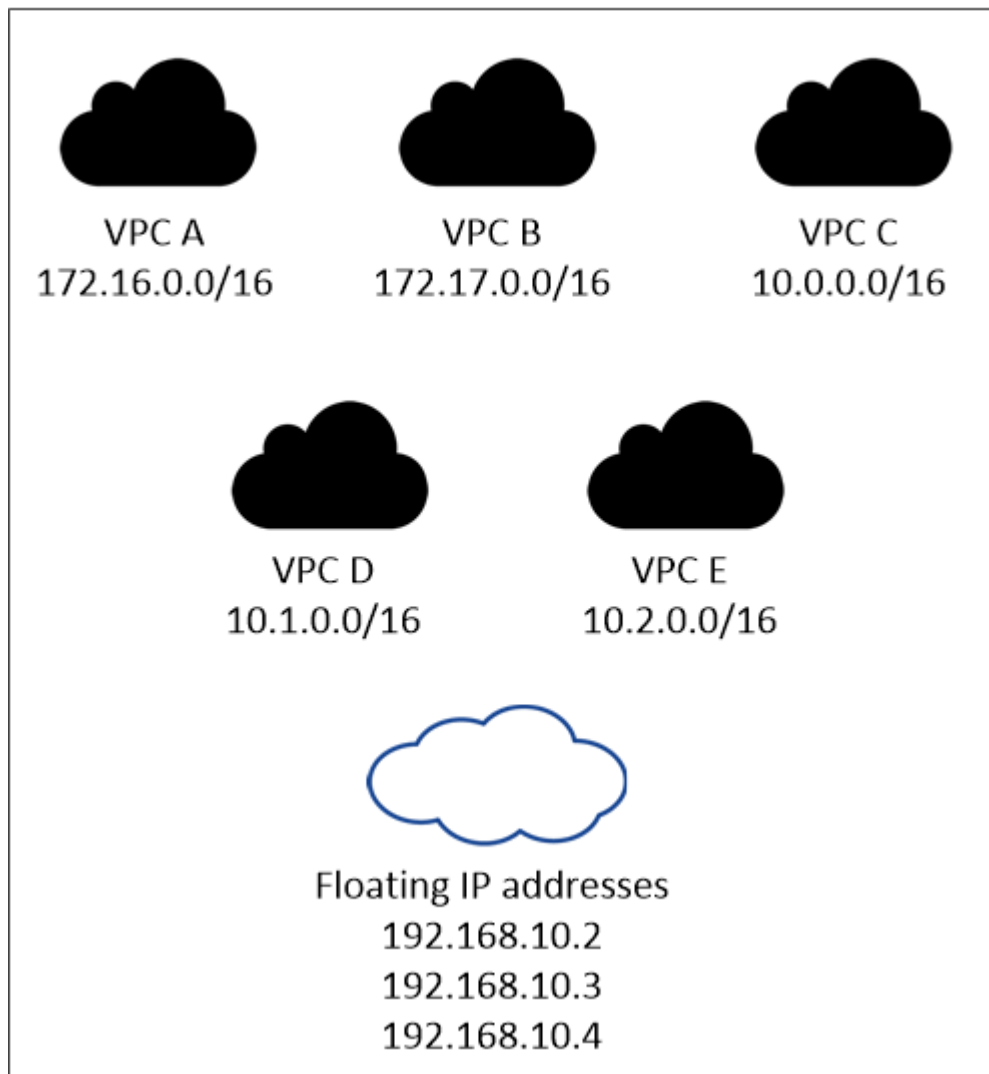
Se si utilizza SnapDrive per Windows o SnapCenter con la coppia ha, è necessario un indirizzo IP mobile per la LIF di gestione SVM. Se non si specifica l'indirizzo IP durante l'implementazione del sistema, è possibile creare la LIF in un secondo momento. Per ulteriori informazioni, vedere "[Configurazione di Cloud Volumes ONTAP](#)".

Quando si crea un ambiente di lavoro Cloud Volumes ONTAP ha, è necessario inserire gli indirizzi IP mobili in Cloud Manager. Cloud Manager assegna gli indirizzi IP alla coppia ha quando avvia il sistema.

Gli indirizzi IP mobili devono essere al di fuori dei blocchi CIDR per tutti i VPC nella regione AWS in cui si implementa la configurazione ha. Gli indirizzi IP mobili sono una subnet logica esterna ai VPC della propria regione.

Nell'esempio seguente viene illustrata la relazione tra gli indirizzi IP mobili e i VPC in una regione AWS. Mentre gli indirizzi IP mobili si trovano al di fuori dei blocchi CIDR per tutti i VPC, sono instradabili alle subnet attraverso le tabelle di routing.

### AWS region



Cloud Manager crea automaticamente indirizzi IP statici per l'accesso iSCSI e NAS da client esterni al VPC. Non è necessario soddisfare alcun requisito per questi tipi di indirizzi IP.

## Gateway di transito per abilitare l'accesso IP mobile dall'esterno del VPC

["Configurare un gateway di transito AWS"](#) Per consentire l'accesso agli indirizzi IP mobili di una coppia ha dall'esterno del VPC in cui risiede la coppia ha.

### Tablelle di percorso

Dopo aver specificato gli indirizzi IP mobili in Cloud Manager, è necessario selezionare le tabelle di routing che devono includere i percorsi verso gli indirizzi IP mobili. In questo modo si abilita l'accesso del client alla coppia ha.

Se si dispone di una sola tabella di routing per le subnet nel VPC (la tabella di routing principale), Cloud Manager aggiunge automaticamente gli indirizzi IP mobili alla tabella di routing. Se si dispone di più tabelle di routing, è molto importante selezionare le tabelle di routing corrette quando si avvia la coppia ha. In caso contrario, alcuni client potrebbero non avere accesso a Cloud Volumes ONTAP.

Ad esempio, potrebbero essere presenti due subnet associate a diverse tabelle di routing. Se si seleziona la tabella di route A, ma non la tabella di route B, i client nella subnet associata alla tabella di route A possono accedere alla coppia ha, ma i client nella subnet associata alla tabella di route B.

Per ulteriori informazioni sulle tabelle di percorso, fare riferimento a ["Documentazione AWS: Tabelle di percorso"](#).

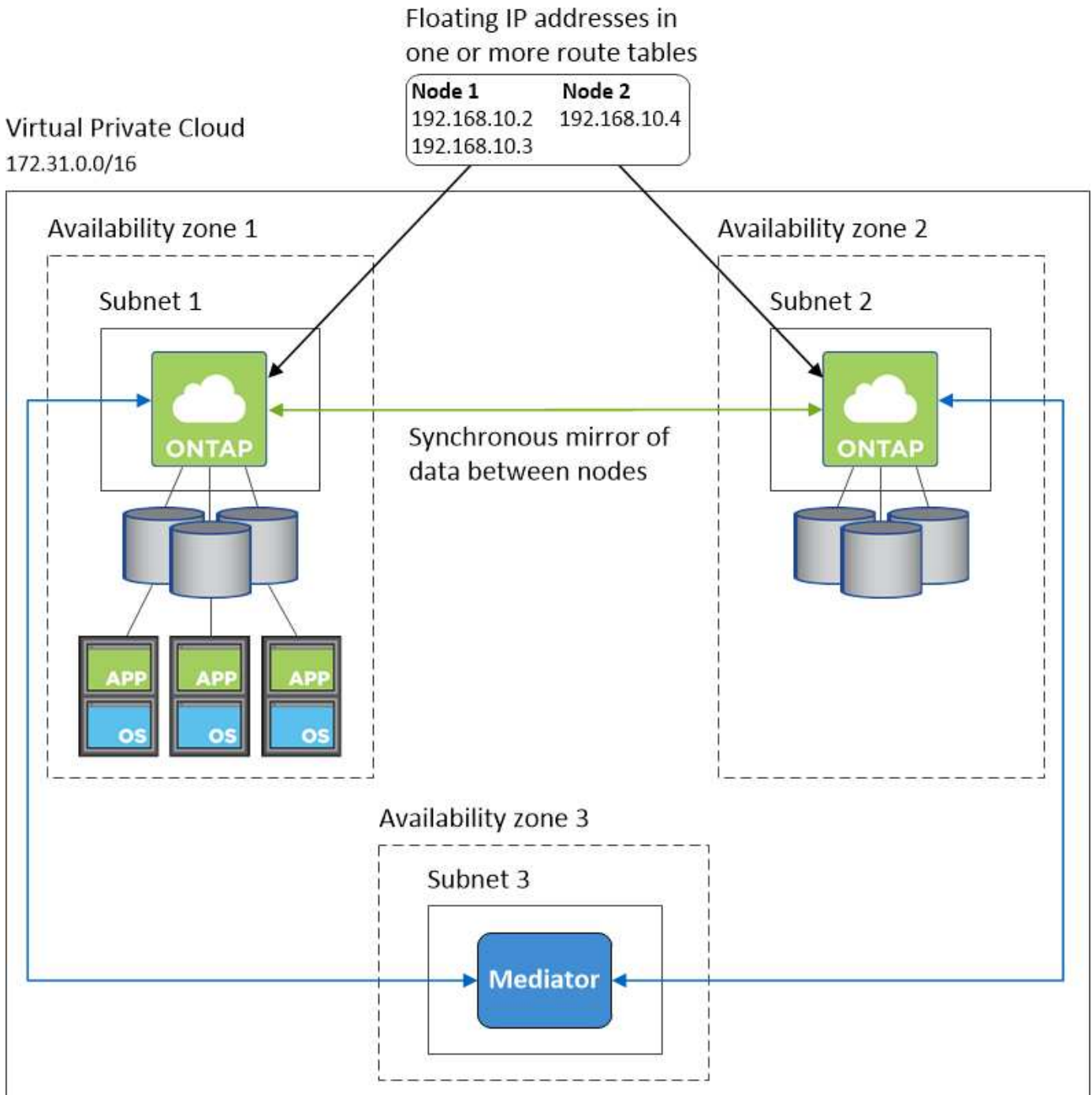
### Connessione ai tool di gestione NetApp

Per utilizzare gli strumenti di gestione NetApp con configurazioni ha che si trovano in più AZS, sono disponibili due opzioni di connessione:

1. Implementare gli strumenti di gestione NetApp in un VPC diverso e ["Configurare un gateway di transito AWS"](#). Il gateway consente l'accesso all'indirizzo IP mobile per l'interfaccia di gestione del cluster dall'esterno del VPC.
2. Implementare gli strumenti di gestione NetApp nello stesso VPC con una configurazione di routing simile a quella dei client NAS.

### Esempio di configurazione ha

La seguente immagine mostra una configurazione ha ottimale in AWS che opera come configurazione Active-passive:



## Requisiti per il connettore

Configura la tua rete in modo che il connettore possa gestire risorse e processi all'interno del tuo ambiente di cloud pubblico. Il passaggio più importante è garantire l'accesso a Internet in uscita a vari endpoint.



Se la rete utilizza un server proxy per tutte le comunicazioni a Internet, è possibile specificare il server proxy dalla pagina Impostazioni. Fare riferimento a ["Configurazione del connettore per l'utilizzo di un server proxy"](#).

## Connessione alle reti di destinazione

Un connettore richiede una connessione di rete ai VPC e ai VNet in cui si desidera implementare Cloud

Volumes ONTAP.

Ad esempio, se si installa un connettore nella rete aziendale, è necessario impostare una connessione VPN a VPC o VNET in cui si avvia Cloud Volumes ONTAP.

### Accesso a Internet in uscita

Il connettore richiede l'accesso a Internet in uscita per gestire risorse e processi all'interno del tuo ambiente di cloud pubblico. Un connettore contatta i seguenti endpoint durante la gestione delle risorse in AWS:

Endpoint	Scopo
Servizi AWS (amazonaws.com): <ul style="list-style-type: none"><li>• CloudFormation</li><li>• Elastic Compute Cloud (EC2)</li><li>• Servizio di gestione delle chiavi (KMS)</li><li>• Servizio token di sicurezza (STS)</li><li>• S3 (Simple Storage Service)</li></ul> L'endpoint esatto dipende dalla regione in cui viene implementato Cloud Volumes ONTAP. "Per ulteriori informazioni, fare riferimento alla documentazione AWS."	Consente a Cloud Manager di implementare e gestire Cloud Volumes ONTAP in AWS.
<a href="https://api.services.cloud.netapp.com:443">https://api.services.cloud.netapp.com:443</a>	Richieste API a NetApp Cloud Central.
<a href="https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com">https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com</a>	Fornisce l'accesso a immagini, manifesti e modelli software.
<a href="https://repo.cloud.support.netapp.com">https://repo.cloud.support.netapp.com</a>	Utilizzato per scaricare le dipendenze di Cloud Manager.
<a href="http://repo.mysql.com/">http://repo.mysql.com/</a>	Utilizzato per scaricare MySQL.
<a href="https://cognito-idp.us-east-1.amazonaws.com">https://cognito-idp.us-east-1.amazonaws.com</a> <a href="https://cognito-identity.us-east-1.amazonaws.com">https://cognito-identity.us-east-1.amazonaws.com</a> <a href="https://sts.amazonaws.com">https://sts.amazonaws.com</a> <a href="https://cloud-support-netapp-com-accelerated.s3.amazonaws.com">https://cloud-support-netapp-com-accelerated.s3.amazonaws.com</a>	Consente a Cloud Manager di accedere e scaricare manifesti, modelli e immagini di aggiornamento di Cloud Volumes ONTAP.
<a href="https://cloudmanagerinfraprod.azurecr.io">https://cloudmanagerinfraprod.azurecr.io</a>	Accesso alle immagini software dei componenti container per un'infrastruttura che esegue Docker e fornisce una soluzione per l'integrazione dei servizi con Cloud Manager.
<a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a>	Consente a NetApp di eseguire lo streaming dei dati dai record di audit.
<a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a>	Comunicazione con il servizio Cloud Manager, che include gli account Cloud Central.
<a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a>	Comunicazione con NetApp Cloud Central per l'autenticazione utente centralizzata.
<a href="https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist">https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist</a>	Consente di aggiungere l'ID account AWS all'elenco degli utenti autorizzati per Backup in S3.



Endpoint	Scopo
<a href="https://support.netapp.com/aods/asupmessage">https://support.netapp.com/aods/asupmessage</a> <a href="https://support.netapp.com/asupprod/post/1.0/postAsup">https://support.netapp.com/asupprod/post/1.0/postAsup</a>	Comunicazione con NetApp AutoSupport.
<a href="https://support.netapp.com/svcgw">https://support.netapp.com/svcgw</a> <a href="https://support.netapp.com/ServiceGW/entitlement">https://support.netapp.com/ServiceGW/entitlement</a> <a href="https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com">https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com</a> <a href="https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com">https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com</a>	Comunicazione con NetApp per la registrazione del supporto e delle licenze di sistema.
<a href="https://ipa-signer.cloudmanager.netapp.com">https://ipa-signer.cloudmanager.netapp.com</a>	Consente a Cloud Manager di generare licenze (ad esempio, una licenza FlexCache per Cloud Volumes ONTAP)
<a href="https://packages.cloud.google.com/yum">https://packages.cloud.google.com/yum</a> <a href="https://github.com/NetApp/trident/releases/download/">https://github.com/NetApp/trident/releases/download/</a>	Necessario per connettere i sistemi Cloud Volumes ONTAP a un cluster Kubernetes. Gli endpoint consentono l'installazione di NetApp Trident.
<p>Varie sedi di terze parti, ad esempio:</p> <ul style="list-style-type: none"> <li>• <a href="https://repo1.maven.org/maven2">https://repo1.maven.org/maven2</a></li> <li>• <a href="https://oss.sonatype.org/content/repositories">https://oss.sonatype.org/content/repositories</a></li> <li>• <a href="https://repo.typesafe.org">https://repo.typesafe.org</a></li> </ul> <p>Le sedi di terze parti sono soggette a modifiche.</p>	Durante gli aggiornamenti, Cloud Manager scarica i pacchetti più recenti per le dipendenze di terze parti.

Sebbene sia necessario eseguire quasi tutte le attività dall'interfaccia utente SaaS, sul connettore è ancora disponibile un'interfaccia utente locale. Il computer che esegue il browser Web deve disporre di connessioni ai seguenti endpoint:

Endpoint	Scopo
L'host del connettore	<p>Per caricare la console di Cloud Manager, è necessario inserire l'indirizzo IP dell'host da un browser Web.</p> <p>A seconda della connettività con il cloud provider, è possibile utilizzare l'IP privato o un IP pubblico assegnato all'host:</p> <ul style="list-style-type: none"> <li>• Un IP privato funziona se si dispone di una VPN e di un accesso diretto alla rete virtuale</li> <li>• Un IP pubblico funziona in qualsiasi scenario di rete</li> </ul> <p>In ogni caso, è necessario proteggere l'accesso alla rete assicurandosi che le regole del gruppo di protezione consentano l'accesso solo da IP o subnet autorizzati.</p>
<a href="https://auth0.com">https://auth0.com</a> <a href="https://cdn.auth0.com">https://cdn.auth0.com</a> <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> <a href="https://services.cloud.netapp.com">https://services.cloud.netapp.com</a>	Il browser Web si connette a questi endpoint per un'autenticazione utente centralizzata tramite NetApp Cloud Central.

Endpoint	Scopo
<a href="https://widget.intercom.io">https://widget.intercom.io</a>	Per chat in-product che ti consente di parlare con gli esperti cloud di NetApp.

## Configurazione di un gateway di transito AWS per coppie ha in più AZS

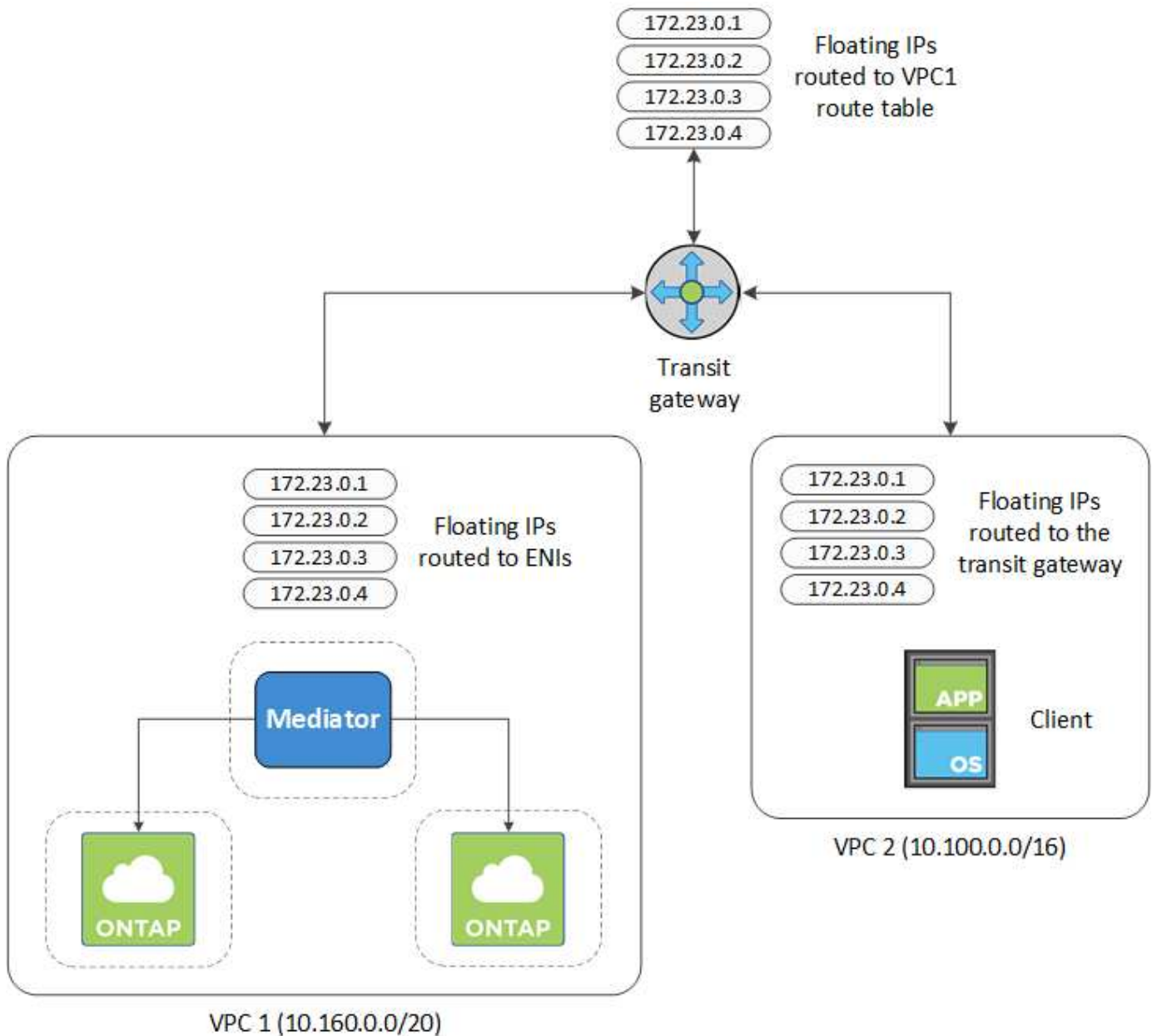
Configurare un gateway di transito AWS per consentire l'accesso a una coppia ha "Indirizzi IP mobili" Dall'esterno del VPC in cui risiede la coppia ha.

Quando una configurazione Cloud Volumes ONTAP ha viene distribuita in più zone di disponibilità AWS, sono richiesti indirizzi IP mobili per l'accesso ai dati NAS dall'interno del VPC. Questi indirizzi IP mobili possono migrare tra i nodi in caso di guasti, ma non sono accessibili in modo nativo dall'esterno del VPC. Gli indirizzi IP privati separati forniscono l'accesso ai dati dall'esterno del VPC, ma non forniscono il failover automatico.

Gli indirizzi IP mobili sono richiesti anche per l'interfaccia di gestione del cluster e per la LIF di gestione SVM opzionale.

Se si imposta un gateway di transito AWS, si abilita l'accesso agli indirizzi IP mobili dall'esterno del VPC in cui risiede la coppia ha. Ciò significa che i client NAS e gli strumenti di gestione NetApp esterni al VPC possono accedere agli IP mobili.

Ecco un esempio che mostra due VPC connessi da un gateway di transito. Un sistema ha risiede in un VPC, mentre un client risiede nell'altro. È quindi possibile montare un volume NAS sul client utilizzando l'indirizzo IP mobile.



La seguente procedura illustra come configurare una configurazione simile.

### Fasi

1. "Creare un gateway di transito e collegare i VPC al gateway".
2. Creare le route nella tabella delle route del gateway di transito specificando gli indirizzi IP mobili della coppia ha.

Gli indirizzi IP mobili sono disponibili nella pagina Working Environment Information (informazioni sull'ambiente di lavoro) di Cloud Manager. Ecco un esempio:

## NFS & CIFS access from within the VPC using Floating IP

### Auto failover

Cluster Management : 172.23.0.1

Data (nfs,cifs) : Node 1: 172.23.0.2 | Node 2: 172.23.0.3

### Access

SVM Management : 172.23.0.4

L'immagine di esempio seguente mostra la tabella di percorso per il gateway di transito. Include le route ai blocchi CIDR dei due VPC e quattro indirizzi IP mobili utilizzati da Cloud Volumes ONTAP.

Transit Gateway Route Table: tgw-rtb-0ea8ee291c7aeddd3

Details Associations Propagations **Routes** Tags

The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.

Create route Replace route Delete route

Filter by attributes or search by keyword

<input type="checkbox"/>	CIDR	Attachment	Resource type	Route type	Route state
<input type="checkbox"/>	10.100.0.0/16	tgw-attach-05e77bd34e2ff91f8   vpc-0b2bc30e0dc8e0db1	VPC2	propagated	active
<input type="checkbox"/>	10.160.0.0/20	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC1	propagated	active
<input type="checkbox"/>	172.23.0.1/32	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC	static	active
<input type="checkbox"/>	172.23.0.2/32	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC	static	active
<input type="checkbox"/>	172.23.0.3/32	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC	static	active
<input type="checkbox"/>	172.23.0.4/32	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC	static	active

**Floating IP Addresses**

3. Modificare la tabella di routing dei VPC che devono accedere agli indirizzi IP mobili.

- Aggiungere voci di routing agli indirizzi IP mobili.
- Aggiungere una voce di percorso al blocco CIDR del VPC in cui risiede la coppia ha.

L'immagine di esempio seguente mostra la tabella di routing per VPC 2, che include i percorsi verso VPC 1 e gli indirizzi IP mobili.

Route Table: rtb-0569a1bd740ed033f

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status	Propagated
10.100.0.0/16	local	active	No
0.0.0.0/0	igw-07250bd01781e67df	active	No
10.160.0.0/20	tgw-015b7c249661ac279	active	No
172.23.0.1/32	tgw-015b7c249661ac279	active	No
172.23.0.2/32	tgw-015b7c249661ac279	active	No
172.23.0.3/32	tgw-015b7c249661ac279	active	No
172.23.0.4/32	tgw-015b7c249661ac279	active	No

VPC1  
Floating IP Addresses

4. Modificare la tabella di routing per il VPC della coppia ha aggiungendo un percorso al VPC che richiede l'accesso agli indirizzi IP mobili.

Questo passaggio è importante perché completa il routing tra i VPC.

L'immagine di esempio seguente mostra la tabella di percorso per VPC 1. Include un routing agli indirizzi IP mobili e a VPC 2, che è dove risiede un client. Cloud Manager ha aggiunto automaticamente gli IP mobili alla tabella di routing quando ha implementato la coppia ha.

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status
10.160.0.0/20	local	active
pl-68a54001 (com.amazonaws.us-west-2.s3, 54.231.160.0/19, 52.218.128.0/17, 52.92.32.0/22)	vpce-cb51a0a2	active
0.0.0.0/0	igw-b2182dd7	active
10.60.29.0/25	pcx-589c3331	active
10.100.0.0/16	tgw-015b7c249661ac279	active
10.129.0.0/20	pcx-ff7e1396	active
172.23.0.1/32	eni-0854d4715559c3cdb	active
172.23.0.2/32	eni-0854d4715559c3cdb	active
172.23.0.3/32	eni-0f76681216c3108ed	active
172.23.0.4/32	eni-0854d4715559c3cdb	active

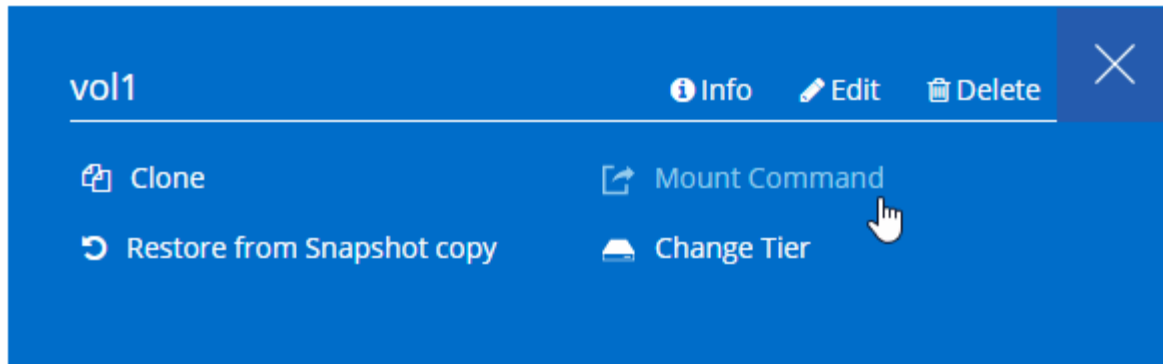
VPC2  
Floating act IP Addresses

5. Montare i volumi sui client utilizzando l'indirizzo IP mobile.

È possibile trovare l'indirizzo IP corretto in Cloud Manager selezionando un volume e facendo clic su **Mount Command**.

# Volumes

2 Volumes | 0.22 TB Allocated | < 0.01 TB Used (0 TB in S3)



## Link correlati

- ["Coppie ad alta disponibilità in AWS"](#)
- ["Requisiti di rete per Cloud Volumes ONTAP in AWS"](#)

## Regole del gruppo di sicurezza per AWS

Cloud Manager crea gruppi di sicurezza AWS che includono le regole in entrata e in uscita necessarie per il corretto funzionamento di Connector e Cloud Volumes ONTAP. È possibile fare riferimento alle porte a scopo di test o se si preferisce utilizzare i propri gruppi di protezione.

### Regole per Cloud Volumes ONTAP

Il gruppo di sicurezza per Cloud Volumes ONTAP richiede regole sia in entrata che in uscita.

#### Regole in entrata

L'origine delle regole in entrata nel gruppo di sicurezza predefinito è 0.0.0.0/0.

Protocollo	Porta	Scopo
Tutti gli ICMP	Tutto	Eseguire il ping dell'istanza
HTTP	80	Accesso HTTP alla console Web di System Manager utilizzando l'indirizzo IP della LIF di gestione del cluster
HTTPS	443	Accesso HTTPS alla console Web di System Manager utilizzando l'indirizzo IP della LIF di gestione del cluster
SSH	22	Accesso SSH all'indirizzo IP della LIF di gestione del cluster o di una LIF di gestione dei nodi

Protocollo	Porta	Scopo
TCP	111	Chiamata a procedura remota per NFS
TCP	139	Sessione del servizio NetBIOS per CIFS
TCP	161-162	Protocollo di gestione di rete semplice
TCP	445	Microsoft SMB/CIFS su TCP con frame NetBIOS
TCP	635	Montaggio NFS
TCP	749	Kerberos
TCP	2049	Daemon del server NFS
TCP	3260	Accesso iSCSI tramite LIF dei dati iSCSI
TCP	4045	Daemon di blocco NFS
TCP	4046	Network status monitor per NFS
TCP	10000	Backup con NDMP
TCP	11104	Gestione delle sessioni di comunicazione tra cluster per SnapMirror
TCP	11105	Trasferimento dei dati SnapMirror con LIF intercluster
UDP	111	Chiamata a procedura remota per NFS
UDP	161-162	Protocollo di gestione di rete semplice
UDP	635	Montaggio NFS
UDP	2049	Daemon del server NFS
UDP	4045	Daemon di blocco NFS
UDP	4046	Network status monitor per NFS
UDP	4049	Protocollo NFS rquotad

### Regole in uscita

Il gruppo di protezione predefinito per Cloud Volumes ONTAP apre tutto il traffico in uscita. Se questo è accettabile, attenersi alle regole di base per le chiamate in uscita. Se sono necessarie regole più rigide, utilizzare le regole avanzate in uscita.

### Regole di base in uscita

Il gruppo di protezione predefinito per Cloud Volumes ONTAP include le seguenti regole in uscita.

Protocollo	Porta	Scopo
Tutti gli ICMP	Tutto	Tutto il traffico in uscita
Tutti i TCP	Tutto	Tutto il traffico in uscita
Tutti gli UDP	Tutto	Tutto il traffico in uscita

### Regole avanzate in uscita

Se sono necessarie regole rigide per il traffico in uscita, è possibile utilizzare le seguenti informazioni per aprire solo le porte richieste per le comunicazioni in uscita da Cloud Volumes ONTAP.



L'origine è l'interfaccia (indirizzo IP) del sistema Cloud Volumes ONTAP.



Servizio	Protocollo	Porta	Origine	Destinazione	Scopo	
Active Directory	TCP	88	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Autenticazione Kerberos V.	
	UDP	137	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Servizio nomi NetBIOS	
	UDP	138	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Servizio datagramma NetBIOS	
	TCP	139	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Sessione del servizio NetBIOS	
	TCP E UDP	389	LIF di gestione dei nodi	Insieme di strutture di Active Directory	LDAP	
	TCP	445	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Microsoft SMB/CIFS su TCP con frame NetBIOS	
	TCP	464	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Kerberos V change & set password (SET_CHANGE)	
	UDP	464	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Amministrazione delle chiavi Kerberos	
	TCP	749	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Kerberos V change & set Password (RPCSEC_GSS)	
	TCP	88	Data LIF (NFS, CIFS, iSCSI)	Insieme di strutture di Active Directory	Autenticazione Kerberos V.	
	UDP	137	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Servizio nomi NetBIOS	
	UDP	138	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Servizio datagramma NetBIOS	
	TCP	139	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Sessione del servizio NetBIOS	
	TCP E UDP	389	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	LDAP	
	TCP	445	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Microsoft SMB/CIFS su TCP con frame NetBIOS	
	TCP	464	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Kerberos V change & set password (SET_CHANGE)	
	UDP	464	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Amministrazione delle chiavi Kerberos	
	TCP	749	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Kerberos V change & set password (RPCSEC_GSS)	
	Backup su S3	TCP	5010	LIF intercluster	Endpoint di backup o endpoint di ripristino	Operazioni di backup e ripristino per la funzione Backup in S3

Servizio	Protocollo	Porta	Origine	Destinazione	Scopo
Cluster	Tutto il traffico	Tutto il traffico	Tutte le LIF su un nodo	Tutte le LIF sull'altro nodo	Comunicazioni tra cluster (solo Cloud Volumes ONTAP ha)
	TCP	3000	LIF di gestione dei nodi	MEDIATORE HA	Chiamate ZAPI (solo Cloud Volumes ONTAP ha)
	ICMP	1	LIF di gestione dei nodi	MEDIATORE HA	Mantieni attivo (solo Cloud Volumes ONTAP ha)
DHCP	UDP	68	LIF di gestione dei nodi	DHCP	Client DHCP per la prima installazione
DHCPS	UDP	67	LIF di gestione dei nodi	DHCP	Server DHCP
DNS	UDP	53	LIF di gestione dei nodi e LIF dei dati (NFS, CIFS)	DNS	DNS
NDMP	TCP	1860-18699	LIF di gestione dei nodi	Server di destinazione	Copia NDMP
SMTP	TCP	25	LIF di gestione dei nodi	Server di posta	Gli avvisi SMTP possono essere utilizzati per AutoSupport
SNMP	TCP	161	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	UDP	161	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	TCP	162	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	UDP	162	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
SnapMirror	TCP	11104	LIF intercluster	ONTAP Intercluster LIF	Gestione delle sessioni di comunicazione tra cluster per SnapMirror
	TCP	11105	LIF intercluster	ONTAP Intercluster LIF	Trasferimento dei dati SnapMirror
Syslog	UDP	514	LIF di gestione dei nodi	Server syslog	Messaggi di inoltro syslog

## Regole per il gruppo di sicurezza esterno del mediatore ha

Il gruppo di sicurezza esterno predefinito per il mediatore Cloud Volumes ONTAP ha include le seguenti regole in entrata e in uscita.

## Regole in entrata

L'origine delle regole in entrata è 0.0.0.0/0.

Protocollo	Porta	Scopo
SSH	22	Connessioni SSH al mediatore ha
TCP	3000	Accesso API RESTful dal connettore

## Regole in uscita

Il gruppo di sicurezza predefinito per il mediatore ha apre tutto il traffico in uscita. Se questo è accettabile, attenersi alle regole di base per le chiamate in uscita. Se sono necessarie regole più rigide, utilizzare le regole avanzate in uscita.

### Regole di base in uscita

Il gruppo di protezione predefinito per il mediatore ha include le seguenti regole in uscita.

Protocollo	Porta	Scopo
Tutti i TCP	Tutto	Tutto il traffico in uscita
Tutti gli UDP	Tutto	Tutto il traffico in uscita

### Regole avanzate in uscita

Se sono necessarie regole rigide per il traffico in uscita, è possibile utilizzare le seguenti informazioni per aprire solo le porte necessarie per la comunicazione in uscita dal mediatore ha.

Protocollo	Porta	Destinazione	Scopo
HTTP	80	Indirizzo IP del connettore	Scarica gli aggiornamenti per il mediatore
HTTPS	443	Servizi API AWS	Assistenza per il failover dello storage
UDP	53	Servizi API AWS	Assistenza per il failover dello storage



Anziché aprire le porte 443 e 53, è possibile creare un endpoint VPC di interfaccia dalla subnet di destinazione al servizio AWS EC2.

## Regole per il gruppo di sicurezza interno del mediatore ha

Il gruppo di sicurezza interno predefinito per il mediatore ha Cloud Volumes ONTAP include le seguenti regole. Cloud Manager crea sempre questo gruppo di sicurezza. Non hai la possibilità di utilizzare il tuo.

### Regole in entrata

Il gruppo di sicurezza predefinito include le seguenti regole in entrata.

Protocollo	Porta	Scopo
Tutto il traffico	Tutto	Comunicazione tra il mediatore ha e i nodi ha

## Regole in uscita

Il gruppo di protezione predefinito include le seguenti regole in uscita.

Protocollo	Porta	Scopo
Tutto il traffico	Tutto	Comunicazione tra il mediatore ha e i nodi ha

## Regole per il connettore

Il gruppo di protezione per il connettore richiede regole sia in entrata che in uscita.

### Regole in entrata

L'origine delle regole in entrata nel gruppo di sicurezza predefinito è 0.0.0.0/0.

Protocollo	Porta	Scopo
SSH	22	Fornisce l'accesso SSH all'host del connettore
HTTP	80	Fornisce l'accesso HTTP dai browser Web client all'interfaccia utente locale e alle connessioni da Cloud Compliance
HTTPS	443	Fornisce l'accesso HTTPS dai browser Web client all'interfaccia utente locale
TCP	3128	Fornisce all'istanza Cloud Compliance l'accesso a Internet, se la rete AWS non utilizza un NAT o un proxy

## Regole in uscita

Il gruppo di protezione predefinito per il connettore apre tutto il traffico in uscita. Se questo è accettabile, attenersi alle regole di base per le chiamate in uscita. Se sono necessarie regole più rigide, utilizzare le regole avanzate in uscita.

### Regole di base in uscita

Il gruppo di protezione predefinito per il connettore include le seguenti regole in uscita.

Protocollo	Porta	Scopo
Tutti i TCP	Tutto	Tutto il traffico in uscita
Tutti gli UDP	Tutto	Tutto il traffico in uscita

### Regole avanzate in uscita

Se sono necessarie regole rigide per il traffico in uscita, è possibile utilizzare le seguenti informazioni per aprire solo le porte richieste per la comunicazione in uscita dal connettore.



L'indirizzo IP di origine è l'host del connettore.

<b>Servizio</b>	<b>Protocollo</b>	<b>Porta</b>	<b>Destinazione</b>	<b>Scopo</b>
Active Directory	TCP	88	Insieme di strutture di Active Directory	Autenticazione Kerberos V.
	TCP	139	Insieme di strutture di Active Directory	Sessione del servizio NetBIOS
	TCP	389	Insieme di strutture di Active Directory	LDAP
	TCP	445	Insieme di strutture di Active Directory	Microsoft SMB/CIFS su TCP con frame NetBIOS
	TCP	464	Insieme di strutture di Active Directory	Kerberos V change & set password (SET_CHANGE)
	TCP	749	Insieme di strutture di Active Directory	Modifica e impostazione della password Kerberos V di Active Directory (RPCSEC_GSS)
	UDP	137	Insieme di strutture di Active Directory	Servizio nomi NetBIOS
	UDP	138	Insieme di strutture di Active Directory	Servizio datagramma NetBIOS
	UDP	464	Insieme di strutture di Active Directory	Amministrazione delle chiavi Kerberos
Chiamate API e AutoSupport	HTTPS	443	LIF gestione cluster ONTAP e Internet in uscita	Chiamate API ad AWS e ONTAP e invio di messaggi AutoSupport a NetApp
Chiamate API	TCP	3000	LIF gestione cluster ONTAP	Chiamate API a ONTAP
	TCP	8088	Backup su S3	API chiama il backup in S3
DNS	UDP	53	DNS	Utilizzato per la risoluzione DNS da parte di Cloud Manager
Conformità al cloud	HTTP	80	Istanza di Cloud Compliance	Conformità del cloud per Cloud Volumes ONTAP

## Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

## Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.